Fehlerbehebung bei unbehandelten FMC-Ereignissen und häufigem Abfluss von Ereignisstatusüberwachungswarnungen

Inhalt

Einleitung

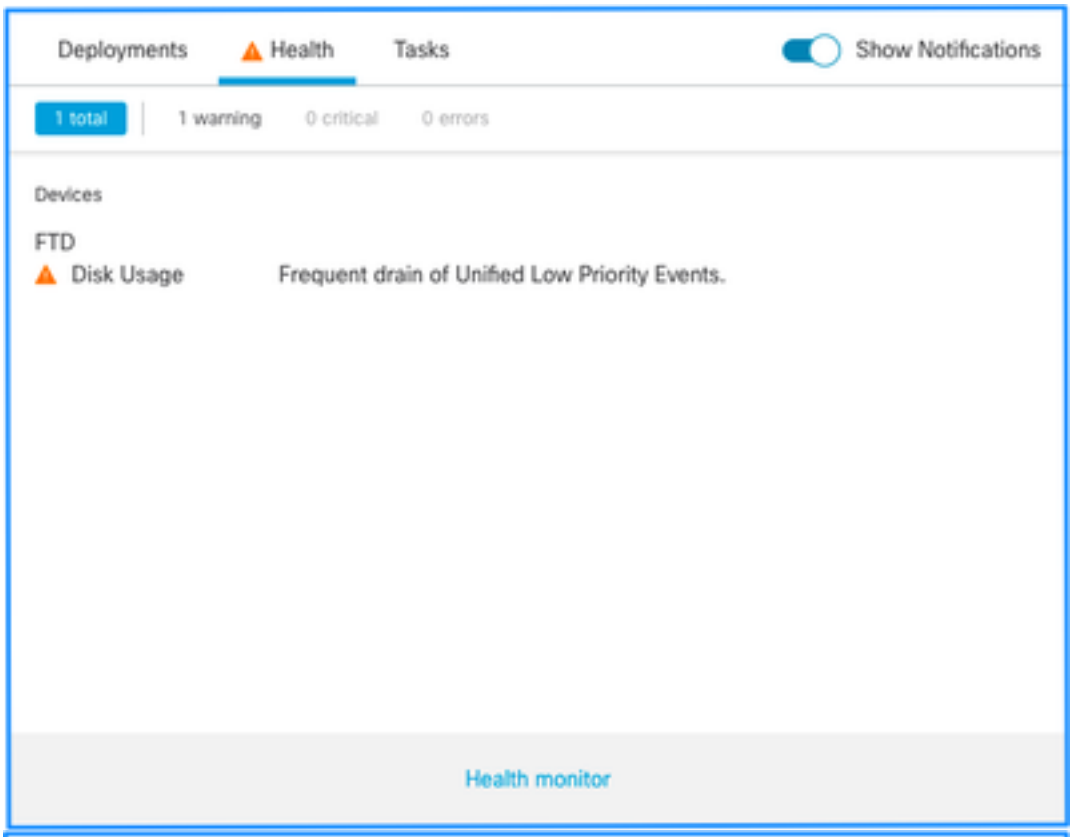
In diesem Dokument wird die Fehlerbehebung bei **nicht verarbeiteten Ereignissen** und **bei häufigen Ereignisablaufwarnungen** im FirePOWER Management Center (FMC) beschrieben.

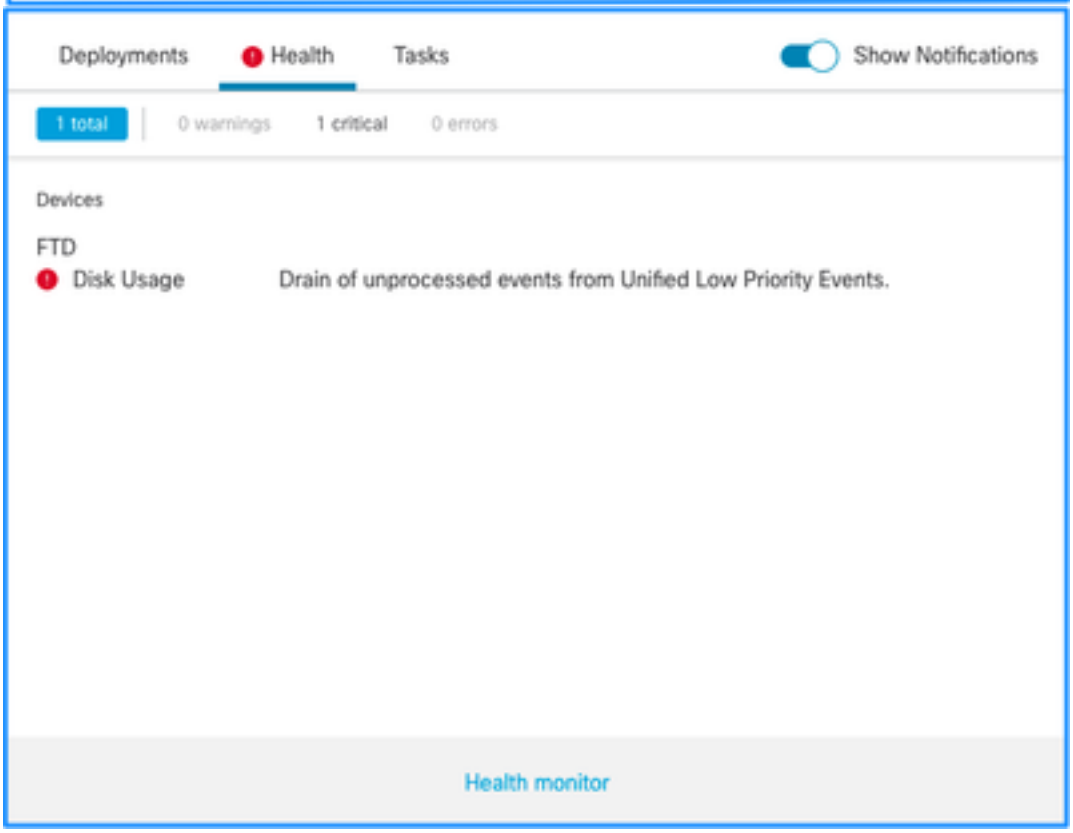
Problemübersicht

Das FMC generiert eine der folgenden Statuswarnungen:

- Häufige Abwanderung von Unified Low Priority-Ereignissen
  und/oder
- Ableitung nicht verarbeiteter Ereignisse aus Unified-Ereignissen mit niedriger Priorität

Obwohl diese Ereignisse generiert und auf dem FMC angezeigt werden, beziehen sie sich auf einen verwalteten Gerätesensor, egal ob es sich um ein FTD-Gerät (Firepower Threat Defense) oder ein NGIPS-Gerät (Intrusion Prevention System der nächsten Generation) handelt. Im weiteren Verlauf dieses Dokuments bezieht sich der Begriff Sensor auf FTD- und NGIPS-Geräte gleichermaßen, sofern nicht anders angegeben.





Dies ist die Struktur der Integritätswarnungen:

- Häufiger Abfluss von <SILO NAME>
- Nicht verarbeitete Ereignisse werden aus <SILO NAME> abgeleitet.

In diesem Beispiel ist SILO NAME **Unified Low Priority Events**. Dies ist eines der isolierten Bereiche des Datenträgermanagers (weitere Informationen finden Sie im Abschnitt Hintergrundinformationen).

Zusätzlich:

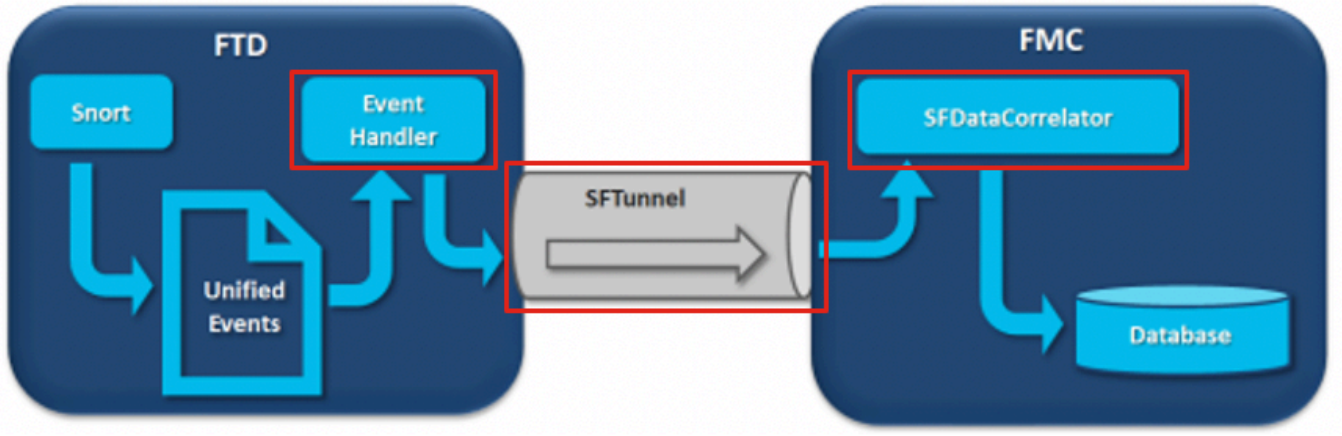
- Obwohl jedes Silo technisch gesehen eine häufige Abnahme von <SILO NAME> Statusmeldungen erzeugen kann, sind die am häufigsten beobachteten Ereignisse Ereignisse, die mit Ereignissen in Zusammenhang stehen, und darunter die Ereignisse mit niedriger Priorität, einfach weil diese die Art von Ereignissen sind, die häufiger von den Sensoren generiert werden.
- Ein "Frequent Drain of <SILO NAME>"-Ereignis hat einen Warnschweregrad, wenn es sich um ein ereignisbezogenes Silo handelt, da es, wenn dieses Ereignis verarbeitet wurde (eine Erklärung darüber, was ein nicht verarbeitetes Ereignis darstellt, wird als Nächstes gegeben), in der FMC-Datenbank vorhanden ist.
- Bei einem nicht ereignisbezogenen Silo, wie dem Silo "Backups", ist die Warnmeldung "Kritisch", da diese Informationen verloren gehen.
- Nur silos von Ereignistypen generieren eine Ableitung nicht verarbeiteter Ereignisse aus der <SILO NAME> Integritätswarnung. Dieser Alarm hat immer den Schweregrad Kritisch.

Weitere Symptome können sein:

- Langsamkeit auf der Benutzeroberfläche des FÜZ
- Veranstaltungsausfall

Häufige Fehlerbehebungsszenarien

Häufige Verluste von <SILO NAME> werden durch zu viele Eingaben in das Silo verursacht. In diesem Fall leert (löscht) der Datenträgermanager diese Datei mindestens zweimal im letzten 5-Minuten-Intervall. In einem Ereignistypsilo wird dies normalerweise durch übermäßige Protokollierung dieses Ereignistyps verursacht. Im Fall eines "Drain of unprocessing events" (Abfluss nicht verarbeiteter Ereignisse) der <SILO NAME>-Integritätswarnung kann dies auch durch einen Engpass im Ereignisverarbeitungspfad verursacht werden.



Das Diagramm enthält drei mögliche Engpässe:

- Der EventHandler-Prozess auf FTD ist überbelegt (er liest langsamer als Snort schreibt)
- Die Eventing-Schnittstelle ist überbelegt.
- Der SFDataCorrelator-Prozess auf FMC ist überbelegt.

Weitere Informationen zur Architektur der Ereignisverarbeitung finden Sie im entsprechenden

Abschnitt mit den Details.

Fall 1: Übermäßige Protokollierung

Wie im vorherigen Abschnitt erwähnt, besteht eine der häufigsten Ursachen für diese Art von Systemwarnungen in übermäßiger Eingabe.

Der Unterschied zwischen der Niedrigwassermarke (LWM) und der Hochwassermarke (HWM), die mit dem CLISH-Befehl **show disk-manager** gesammelt wurde, zeigt, wie viel Platz in diesem Silo benötigt wird, um von LWM (frisch entwässert) zum HWM-Wert zu gelangen. Bei häufigen Ablaufterminen (mit oder ohne nicht verarbeitete Ereignisse) müssen Sie zuerst die Protokollierungskonfiguration überprüfen.

Eine ausführliche Erläuterung des Disk Manager-Prozesses finden Sie im entsprechenden Abschnitt Deep Dive.

Unabhängig davon, ob es sich um eine doppelte Protokollierung oder nur um eine hohe Ereignisrate im gesamten Manager-Sensoren-Ökosystem handelt, müssen die Protokollierungseinstellungen überprüft werden.

Empfohlene Maßnahmen

Schritt 1: Überprüfen auf Doppelprotokollierung

Szenarien mit doppelter Protokollierung können identifiziert werden, wenn Sie sich die **Korrelator**-Perfstats auf dem FMC ansehen, wie in der folgenden Ausgabe dargestellt:

```
admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
129 statistics lines read
                host limit:                     50000           0               50000
                pcnt host limit in use:         0.01            0.01            0.01
                rna events/second:              0.00            0.00            0.06
                user cpu time:                  0.48            0.21            10.09
                system cpu time:                0.47            0.00            8.83
                memory usage:                   2547304         0               2547304
                resident memory usage:          28201           0               49736
                 rna flows/second:               126.41          0.00            3844.16
                 rna dup flows/second:           69.71           0.00            2181.81
                 ids alerts/second:              0.00            0.00            0.00
                ids packets/second:             0.00            0.00            0.00
                ids comm records/second:        0.02            0.01            0.03
                ids extras/second:              0.00            0.00            0.00
                fw_stats/second:                0.00            0.00            0.03
                user logins/second:             0.00            0.00            0.00
                file events/second:             0.00            0.00            0.00
                malware events/second:          0.00            0.00            0.00
                fireamp events/second:          0.00            0.00            0.00
```

In diesem Fall ist eine hohe Rate duplizierter Ströme in der Ausgabe zu sehen.

Schritt 2: Überprüfen der Protokolleinstellungen des ACP

Sie müssen mit einer Überprüfung der Protokolleinstellungen der Zugriffskontrollrichtlinie (Access Control Policy, ACP) beginnen. Befolgen Sie die in diesem Dokument beschriebenen Best Practices für die Verbindungsprotokollierung.

Eine Überprüfung der Protokollierungseinstellungen ist in allen Situationen ratsam, da die aufgeführten Empfehlungen nicht nur Doppelprotokollierungsszenarien abdecken.

Schritt 3: Überprüfen, ob eine übermäßige Protokollierung erwartet wird

Sie müssen überprüfen, ob die übermäßige Protokollierung eine erwartete Ursache hat oder nicht. Wenn die exzessive Protokollierung durch einen DOS/DDoS-Angriff oder einen Routing-Loop oder durch eine bestimmte Anwendung/einen bestimmten Host, die eine große Anzahl von Verbindungen herstellt, verursacht wird, müssen Sie die Verbindungen von den unerwarteten exzessiven Verbindungsquellen überprüfen und abwehren.

Schritt 4: Upgrade-Modell

FTD-Hardwaregerät auf leistungsstärkeres Modell (z. B. FPR2100 —> FPR4100) aktualisieren, da die Anzahl der isolierten Komponenten zunehmen würde.

Schritt 5. Überlegen Sie, ob Sie Log to Ramdisk deaktivieren können

Im Falle des Unified Low Priority Events-Silos können Sie die Option Log to Ramdisk (Ramdisk protokollieren) deaktivieren, um die Silomenge zu vergrößern. Die Nachteile werden im entsprechenden Abschnitt zu den Details erläutert.

Fall 2: Engpass im Kommunikationskanal zwischen Sensor und FMC

Eine weitere häufige Ursache für diese Art von Warnmeldungen sind Verbindungsprobleme und/oder Instabilitäten im Kommunikationskanal (Sftunnel) zwischen dem Sensor und dem FMC. Das Kommunikationsproblem kann folgende Ursachen haben:

- sftunnel ist ausgefallen oder instabil (flaps).
- sftunnel ist überbelegt.

Stellen Sie bei einem Problem mit der Sftunnel-Verbindung sicher, dass das FMC und der Sensor über den TCP-Port 8305 zwischen ihren Verwaltungsschnittstellen erreichbar sind.

Auf FTD können Sie in der Datei **[/ngfw]/var/log/messages nach sftunneld** suchen. Verbindungsprobleme führen dazu, dass Meldungen wie diese generiert werden:

```
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_ch_util [INFO] Delay for heartbeat
reply on channel from 10.62.148.75 for 609 seconds. dropChannel...
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_connections [INFO] Ping Event
Channel for 10.62.148.75 failed
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_channel [INFO] >> ChannelState
dropChannel peer 10.62.148.75 / channelB / EVENT [ msgSock2 & ssl_context2 ] <<
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_channel [INFO] >> ChannelState
freeChannel peer 10.62.148.75 / channelB / DROPPED [ msgSock2 & ssl_context2 ] <<
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_connections [INFO] Need to send SW
version and Published Services to 10.62.148.75
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_peers [INFO] Confirm RPC service in
CONTROL channel
Sep  9 15:41:35 firepower SF-IMS[5458]: [27602] sftunneld:sf_channel [INFO] >> ChannelState
do_dataio_for_heartbeat peer 10.62.148.75 / channelA / CONTROL [ msgSock & ssl_context ] <<
Sep  9 15:41:48 firepower SF-IMS[5458]: [5464] sftunneld:tunnsockets [INFO] Started listening on
port 8305 IPv4(10.62.148.180) management0
Sep  9 15:41:51 firepower SF-IMS[5458]: [27602] sftunneld:control_services [INFO] Successfully
Send Interfaces info to peer 10.62.148.75 over managemen
```

```
Sep  9 15:41:53 firepower SF-IMS[5458]: [5465] sftunneld:sf_connections [INFO] Start connection
to : 10.62.148.75 (wait 10 seconds is up)
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_peers [INFO] Peer 10.62.148.75
needs the second connection
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_ssl [INFO] Interface management0 is
configured for events on this Device
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_ssl [INFO] Connect to 10.62.148.75
on port 8305 - management0
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_ssl [INFO] Initiate IPv4 connection
to 10.62.148.75 (via management0)
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_ssl [INFO] Initiating IPv4
connection to 10.62.148.75:8305/tcp
Sep  9 15:41:53 firepower SF-IMS[5458]: [27061] sftunneld:sf_ssl [INFO] Wait to connect to 8305
(IPv6): 10.62.148.75
```

Eine Überbelegung der Verwaltungsschnittstelle des FMC kann eine Spitze des Verwaltungsdatenverkehrs oder eine konstante Überbelegung sein. Verlaufsdaten des Gesundheitsmonitors sind ein guter Indikator dafür.

Zunächst ist zu beachten, dass das FMC in den meisten Fällen mit einer einzigen NIC für die Verwaltung bereitgestellt wird. Diese Schnittstelle wird verwendet für:

- FMC-Management.
- FMC Sensor Management
- Erfassung von FMC-Ereignissen von den Sensoren.
- Aktualisierung von Intelligence Feeds.
- Herunterladen von SRU-, Software-, VDB- und GeoDB-Updates von der Software-Download-Site
- Die Abfrage für URL-Reputationen und -Kategorien (falls zutreffend).
- Die Abfrage für Dateieinblendungen (falls zutreffend).

Empfohlene Maßnahmen

Sie können eine zweite Netzwerkkarte im FMC für eine dedizierte Ereignisschnittstelle bereitstellen. Implementierungen können vom Anwendungsfall abhängen.

Allgemeine Richtlinien finden Sie im FMC Hardware Guide Deploying on a Management Network.

Fall 3: Ein Engpass im SFDataCorrelator-Prozess

Das letzte zu behandelnde Szenario tritt auf, wenn der Engpass auf der Seite des SFDataCorrelator (FMC) auftritt.

Der erste Schritt besteht darin, sich die Datei diskmanager.log anzusehen, da wichtige Informationen wie die folgenden gesammelt werden müssen:

- Die Frequenz des Drains.
- Die Anzahl der Dateien mit abgelaufenen nicht verarbeiteten Ereignissen.
- Das Auftreten des Drains mit nicht verarbeiteten Ereignissen.

Informationen zur Datei diskmanager.log und deren Interpretation finden Sie im Abschnitt Datenträgerverwaltung. Die Informationen aus der Datei diskmanager.log können dazu verwendet werden, die nachfolgenden Schritte einzugrenzen.

Zusätzlich müssen Sie sich die entsprechenden Leistungsstatistiken ansehen:

```
admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
129 statistics lines read
host limit: 50000 0 50000 pcnt host limit in use: 100.01 100.00 100.55 rna events/second: 1.78
0.00 48.65 user cpu time: 2.14 0.11 58.20 system cpu time: 1.74 0.00 41.13 memory usage: 5010148
0 5138904 resident memory usage: 757165 0 900792                  rna flows/second:
101.90           0.00            3388.23
                 rna dup flows/second:              0.00            0.00            0.00
                 ids alerts/second:                 0.00            0.00            0.00
                 ids packets/second:                0.00            0.00            0.00
                 ids comm records/second:           0.02            0.01            0.03
                 ids extras/second:                 0.00            0.00            0.00
                 fw_stats/second:                   0.01            0.00            0.08
                 user logins/second:                0.00            0.00            0.00
                 file events/second:                0.00            0.00            0.00
                 malware events/second:             0.00            0.00            0.00
                 fireamp events/second:             0.00            0.00            0.01
```

Beachten Sie, dass diese Statistiken für das FÜZ gelten und der Summe aller von ihm verwalteten Sensoren entsprechen. Bei Unified-Veranstaltungen mit niedriger Priorität sind Sie hauptsächlich auf der Suche nach:

- Gesamtanzahl an Flows pro Sekunde für jeden Ereignistyp, um eine mögliche Überbelegung des SFDataCorrelator-Prozesses zu bewerten.
- Die beiden in der vorherigen Ausgabe hervorgehobenen Zeilen: **rna flows/second** - Gibt die Rate von Ereignissen mit niedriger Priorität an, die vom SFDataCorrelator verarbeitet werden.**rna dup flows/second** - Gibt die Rate der duplizierten Ereignisse mit niedriger Priorität an, die vom SFDataCorrelator verarbeitet werden. Dies wird durch doppelte Protokollierung generiert, wie im vorherigen Szenario beschrieben.

Auf der Grundlage der Ergebnisse kann der Schluss gezogen werden, dass

- Es gibt keine doppelte Protokollierung, wie durch die RNA-Duplikat-Flüsse/zweite Zeile angegeben.
- In der Zeile rna flows/second ist der Maximum-Wert viel höher als der Average-Wert, sodass die Rate der Ereignisse, die vom SFDataCorrelator-Prozess verarbeitet wurden, einen Spitzenwert aufwies. Dies ist zu erwarten, wenn Sie sich diesen frühen Morgen anschauen, wenn der Arbeitstag Ihrer Benutzer gerade erst begonnen hat, aber im Allgemeinen ist es eine rote Flagge und erfordert weitere Untersuchungen.

Weitere Informationen zum SFDataCorrelator-Prozess finden Sie im Abschnitt Ereignisverarbeitung.

Empfohlene Maßnahmen

Zuerst müssen Sie feststellen, wann die Spitze aufgetreten ist. Dazu müssen Sie sich die Korrelatorstatistiken für jedes 5-minütige Abtastintervall ansehen. Die Informationen aus der Datei diskmanager.log können Ihnen helfen, sich auf den wichtigen Zeitrahmen zu konzentrieren.

> **Tipp:** Leiten Sie die Ausgabe **weniger** über die Pipeline an den Linux-Pager, sodass Sie einfach suchen können.

```
admin@FMC:~$ sudo perfstats -C < /var/sf/rna/correlator-stats/now

<OUTPUT OMITTED FOR READABILITY>
Wed Sep 9 16:01:35 2020 host limit: 50000 pcnt host limit in use: 100.14 rna events/second:
24.33 user cpu time: 7.34 system cpu time: 5.66 memory usage: 5007832 resident memory usage:
797168  rna flows/second:              638.55
                rna dup flows/second:          0.00
                ids alerts/second:             0.00
                ids pkts/second:               0.00
                ids comm records/second:       0.02
                ids extras/second:             0.00
                fw stats/second:               0.00
                user logins/second:            0.00
                file events/second:            0.00
                malware events/second:         0.00
                fireAMP events/second:         0.00


Wed Sep  9 16:06:39 2020
                host limit:                    50000
                pcnt host limit in use:        100.03
                rna events/second:             28.69
                user cpu time:                 16.04
                system cpu time:               11.52
                memory usage:                  5007832
                resident memory usage:         801476
                rna flows/second:              685.65
                rna dup flows/second:          0.00
                ids alerts/second:             0.00
                ids pkts/second:               0.00
                ids comm records/second:       0.01
                ids extras/second:             0.00
                fw stats/second:               0.00
                user logins/second:            0.00
                file events/second:            0.00
                malware events/second:         0.00
                fireAMP events/second:         0.00

Wed Sep  9 16:11:42 2020
                host limit:                    50000
                pcnt host limit in use:        100.01
                rna events/second:             47.51
                user cpu time:                 16.33
                system cpu time:               12.64
                memory usage:                  5007832
                resident memory usage:         809528
                rna flows/second:              1488.17
                rna dup flows/second:          0.00
                ids alerts/second:             0.00
                ids pkts/second:               0.00
                ids comm records/second:       0.02
                ids extras/second:             0.00
                fw stats/second:               0.01
                user logins/second:            0.00
                file events/second:            0.00
                malware events/second:         0.00
                fireAMP events/second:         0.00

Wed Sep  9 16:16:42 2020
                host limit:                    50000
                pcnt host limit in use:        100.00
                rna events/second:             8.57
```

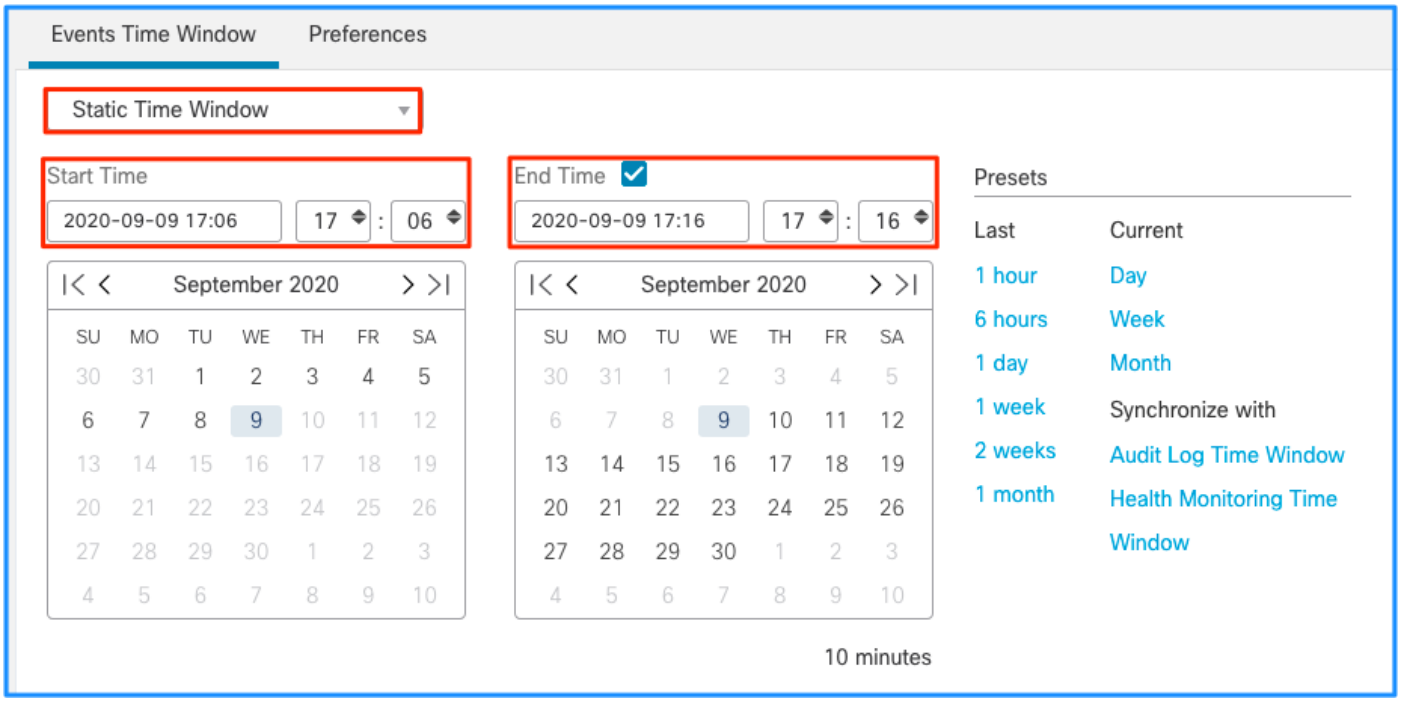
```
user cpu time:                  58.20
system cpu time:                41.13
memory usage:                   5007832
resident memory usage:          837732
rna flows/second:               3388.23
rna dup flows/second:           0.00
ids alerts/second:              0.00
ids pkts/second:                0.00
ids comm records/second:        0.01
ids extras/second:              0.00
fw stats/second:                0.03
user logins/second:             0.00
file events/second:             0.00
malware events/second:          0.00
fireAMP events/second:          0.00

197 statistics lines read

                host limit:                     50000           0               50000
                pcnt host limit in use:         100.01          100.00          100.55
                rna events/second:              1.78            0.00            48.65
                user cpu time:                  2.14            0.11            58.20
                system cpu time:                1.74            0.00            41.13
                memory usage:                   5010148         0               5138904
                resident memory usage:          757165          0               900792
                rna flows/second:               101.90          0.00            3388.23
                rna dup flows/second:           0.00            0.00            0.00
                ids alerts/second:              0.00            0.00            0.00
                ids packets/second:             0.00            0.00            0.00
                ids comm records/second:        0.02            0.01            0.03
                ids extras/second:              0.00            0.00            0.00
                fw_stats/second:                0.01            0.00            0.08
                user logins/second:             0.00            0.00            0.00
                file events/second:             0.00            0.00            0.00
                malware events/second:          0.00            0.00            0.00
                fireamp events/second:          0.00            0.00            0.01
```

Verwenden Sie die Informationen in der Ausgabe, um:

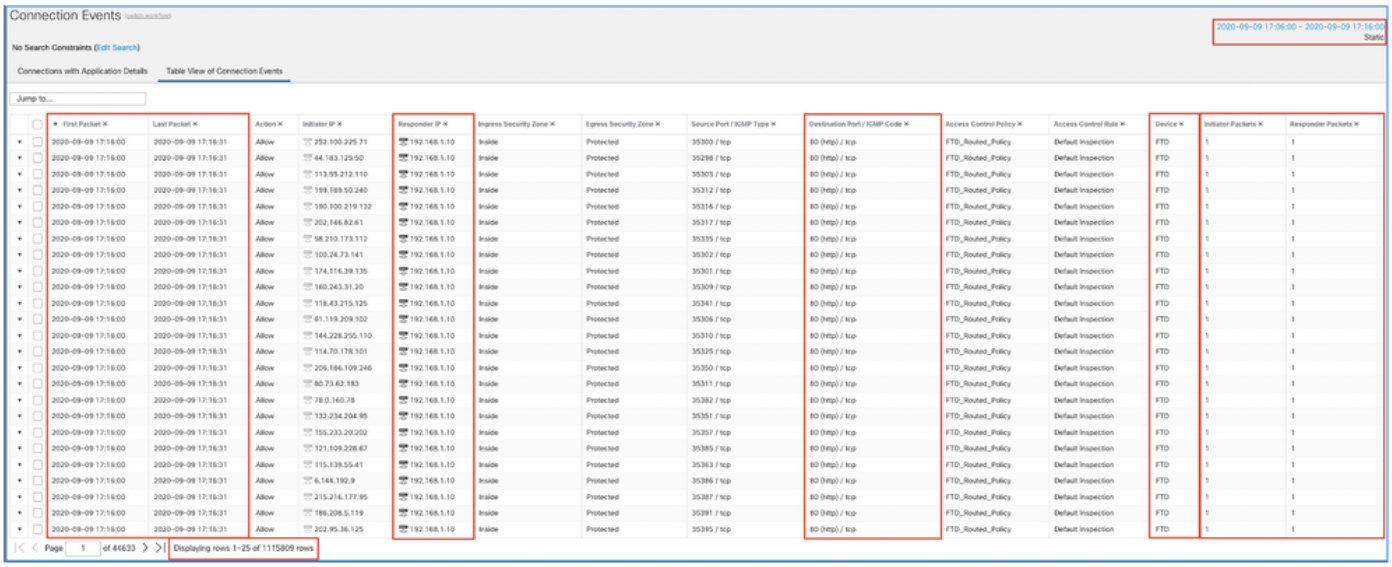
- Ermitteln Sie die normale/Baseline-Rate von Ereignissen.
- Ermitteln Sie das 5-Minuten-Intervall, in dem die Spitze auftrat.

Im vorherigen Beispiel gibt es eine offensichtliche Spitze in der Rate der Ereignisse empfangen um 16:06:39 und darüber hinaus. Beachten Sie, dass es sich hierbei um Durchschnittswerte von 5 Minuten handelt, sodass der Anstieg abrupter als dargestellt ausfallen kann (Burst), aber in diesem 5-Minuten-Intervall verdünnt werden kann, wenn er gegen Ende des Intervalls beginnt.

Obwohl dies zu der Schlussfolgerung führt, dass dieser Ereignisspitzenwert den Ablauf nicht verarbeiteter Ereignisse verursacht hat, können Sie sich die Verbindungsereignisse über die grafische Benutzeroberfläche (GUI) des FMC mit dem entsprechenden Zeitfenster ansehen, um zu verstehen, welche Verbindungstypen die FTD-Box in diesem Spitzenwert durchlaufen haben:



Wenden Sie dieses Zeitfenster an, um die gefilterten Verbindungsereignisse abzurufen. Vergessen Sie nicht, die Zeitzone zu berücksichtigen. In diesem Beispiel verwendet der Sensor UTC und FMC UTC+1. Verwenden Sie die Tabellenansicht, um die Ereignisse anzuzeigen, die die Überlastung der Ereignisse ausgelöst haben, und führen Sie die entsprechenden Maßnahmen aus:



Anhand der Zeitstempel (Zeit des ersten und letzten Pakets) ist zu erkennen, dass es sich um kurzlebige Verbindungen handelt. Darüber hinaus zeigen die Spalten für Initiator- und Responder-Pakete, dass nur ein Paket in jede Richtung ausgetauscht wurde. Dies bestätigt, dass die Verbindungen kurzlebig waren und nur sehr wenig Daten ausgetauscht wurden.

Sie können auch sehen, dass alle diese Flows auf dieselben Responder-IPs und -Ports abzielen. Außerdem werden sie alle vom gleichen Sensor gemeldet (der neben den Schnittstelleninformationen am Eingang und am Ausgang auch den Ort und die Richtung dieser Flüsse anzeigen kann). Zusätzliche Maßnahmen:

- Überprüfen Sie die Syslogs auf dem Zielendpunkt.
- DOS-/DDoS-Schutz implementieren oder andere vorbeugende Maßnahmen ergreifen.

Anmerkung: In diesem Artikel sollen Richtlinien zur Fehlerbehebung bei der Warnung "Ablauf nicht verarbeiteter Ereignisse" angegeben werden. In diesem Beispiel wurde hping3 verwendet, um eine TCP-SYN-Flood zum Zielserver zu generieren. Richtlinien zur Absicherung Ihres FTD-Geräts finden Sie im Cisco Firepower Threat Defense Hardening Guide

Zu sammelnde Artikel, bevor Sie sich an das Cisco Technical Assistance Center (TAC) wenden

Es wird dringend empfohlen, die folgenden Artikel zu sammeln, bevor Sie sich an das Cisco TAC wenden:

- Screenshot der angezeigten Warnmeldungen.
- Fehlerbehebung in der vom FMC generierten Datei
- Fehlerbehebung bei Datei, die vom betroffenen Sensor generiert wurde
- Datum und Uhrzeit, an dem das Problem erstmals aufgetreten ist.
- Informationen zu allen kürzlich vorgenommenen Änderungen an den Richtlinien (falls zutreffend).
- Die Ausgabe des Befehls stats_unified.pl, wie im Abschnitt Ereignisverarbeitung beschrieben, mit einem Hinweis auf die betroffenen Sensoren.

Details

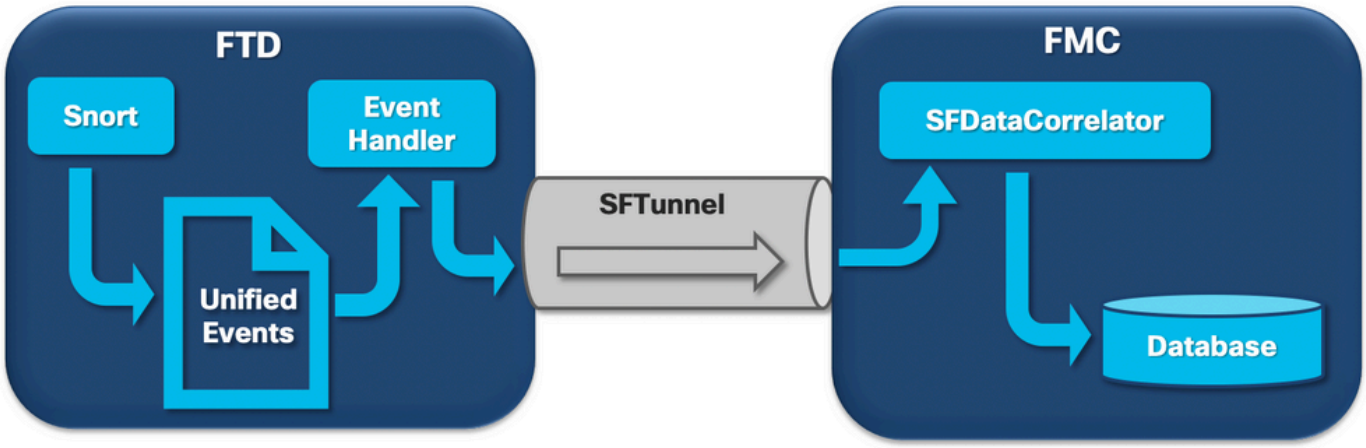
In diesem Abschnitt werden die verschiedenen Komponenten ausführlich erläutert, die an dieser Art von Systemwarnungen beteiligt sein können. Dazu gehören:

- Ereignisverarbeitung - Deckt die Pfadereignisse ab, die auf den Sensorgeräten und dem FMC eingehen. Dies ist vor allem dann nützlich, wenn sich die Integritätswarnung auf einen Ereignistyp "Silo" bezieht.
- Disk Manager - Beschreibt den Prozess der Datenträgerverwaltung, Silos und deren Entleerung.
- Zustandsmonitor - Beschreibt, wie die Zustandsüberwachungsmodule zum Generieren von Zustandswarnungen verwendet werden.
- Log to Ramdisk (Bei Ramdisk anmelden): Beschreibung der Funktion für die Protokollierung bei Ramdisk und ihrer möglichen Auswirkungen auf Statuswarnungen.

Um die Warnmeldungen zum Zustand "Ablauf von Ereignissen" zu verstehen und potenzielle Fehlerpunkte identifizieren zu können, müssen die Funktionsweise dieser Komponenten untersucht und die Interaktion untereinander sichergestellt werden.

Ereignisverarbeitung

Auch wenn die Warnmeldungen zur Art des häufigen Ablaufs durch isolierte Bereiche ausgelöst werden können, die nicht ereignisbezogen sind, bezieht sich die überwiegende Mehrheit der vom Cisco TAC erkannten Fälle auf den Ablauf von ereignisbezogenen Informationen. Um zu verstehen, was eine Abwanderung von nicht verarbeiteten Ereignissen darstellt, ist es außerdem erforderlich, einen Blick auf die Architektur zur Ereignisverarbeitung und die Komponenten zu werfen, aus denen sie besteht.



Wenn ein FirePOWER-Sensor ein Paket von einer neuen Verbindung empfängt, generiert der Snort-Prozess ein Ereignis im Unified2-Format. Dabei handelt es sich um ein Binärformat, das schnellere Lese-/Schreibvorgänge und leichtere Ereignisse ermöglicht.

Die Ausgabe zeigt den FTD-Befehl **system support trace**, wo Sie sehen können, eine neue Verbindung erstellt. Wichtige Teile werden hervorgehoben und erläutert:

```
192.168.0.2-42310 - 192.168.1.10-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3310981951
192.168.0.2-42310 - 192.168.1.10-80 6 AS 1-1 CID 0 Session: new snort session
192.168.0.2-42310 - 192.168.1.10-80 6 AS 1-1 CID 0 AppID: service unknown (0), application
unknown (0)
192.168.0.2-42310 > 192.168.1.10-80 6 AS 1-1 I 0 new firewall session
192.168.0.2-42310 > 192.168.1.10-80 6 AS 1-1 I 0 using HW or preset rule order 4, 'Default
Inspection', action Allow and prefilter rule 0
192.168.0.2-42310 > 192.168.1.10-80 6 AS 1-1 I 0 HitCount data sent for rule id: 268437505,
192.168.0.2-42310 > 192.168.1.10-80 6 AS 1-1 I 0 allow action
192.168.0.2-42310 - 192.168.1.10-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Default Inspection',
allow
192.168.0.2-42310 - 192.168.1.10-80 6 AS 1-1 CID 0 Snort id 0, NAP id 1, IPS id 0, Verdict PASS
```

Snort Unified_events-Dateien werden pro Instanz unter dem Pfad **[/ngfw]var/sf/detection_engine/*/instance-N/** generiert, wobei:

- ***** ist die Snort UUID. Dies ist pro Appliance einzigartig.
- **N** ist die Snort-Instanz-ID, die als Instanz-ID aus der vorherigen Ausgabe berechnet werden kann (im Beispiel die hervorgehobene 0) + 1

Es gibt zwei Arten von Unified_events-Dateien in einem beliebigen Snort-Instanzordner:

- unified_events-1 (enthält Ereignisse mit hoher Priorität).
- unified_events-2 (enthält Ereignisse mit niedriger Priorität).

Ein Ereignis mit hoher Priorität ist ein Ereignis, das einer potenziell schädlichen Verbindung entspricht.

Veranstaltungstypen und ihre Priorität:

Hohe Priorität (1)	Niedrige Priorität (2)
Eindringen	Verbindung
Malware	Erkennung
Sicherheitsinformationen	Datei

Zugehörige Verbindungsereignisse	Statistik

Die nächste Ausgabe zeigt ein Ereignis, das zu der neuen Verbindung gehört, die im vorherigen Beispiel verfolgt wurde. Das Format ist unified2 und wird aus der Ausgabe des jeweiligen Unified-Ereignisprotokolls unter [/ngfw]/var/sf/detection_engine/*/instance-**1/ entnommen,** wobei 1 die fett formatierte Snort-Instanz-ID in der vorherigen Ausgabe +1 ist. Der Name des Unified-Ereignisprotokollformats folgt der Syntax unified_events-**2.**log.**1599 9654750**, wobei 2 für die Priorität der Ereignisse steht, wie in der Tabelle dargestellt, und der letzte fett formatierte Teil (**159654750)** der Zeitstempel (Unix-Zeit) des Erstellens der Datei ist.

> **Tipp:** Sie können den Linux-Befehl **date** verwenden, um die Unix-Zeit in ein lesbares Datum zu konvertieren:
> admin@FP1120-2:~$ **sudo date -d@1599654750**
> Sept. 9 14:32:30 MESZ 2020

```
Unified2 Record at offset 2190389
Type: 210(0x000000d2)
Timestamp: 0
Length: 765 bytes
Forward to DC: Yes
FlowStats:
Sensor ID: 0
Service: 676
NetBIOS Domain: <none>
Client App: 909, Version: 1.20.3 (linux-gnu)
Protocol: TCP
Initiator Port: 42310
Responder Port: 80
First Packet: (1599662092) Tue Sep 9 14:34:52 2020
Last Packet: (1599662092) Tue Sep 9 14:34:52 2020

<OUTPUT OMITTED FOR READABILITY>

Initiator: 192.168.0.2
Responder: 192.168.1.10
Original Client: ::
Policy Revision: 00000000-0000-0000-0000-00005f502a92
Rule ID: 268437505
Tunnel Rule ID: 0
Monitor Rule ID: <none>
Rule Action: 2
```

Neben jeder unified_events-Datei gibt es eine Bookmark-Datei, die 2 wichtige Werte enthält:

1. Zeitstempel, der der aktuellen Datei "unified_events" für diese Instanz und Priorität entspricht.
2. Position in Byte für das letzte Leseereignis in der Datei "unified_event".

Die Werte werden in der folgenden Reihenfolge durch Kommas voneinander getrennt:

```
root@FTD:/home/admin# cat /var/sf/detection_engines/d5a4d5d0-6ddf-11ea-b364-
2ac815c16717/instance-1/unified_events-2.log.bookmark.1a3d52e6-3e09-11ea-838f-68e7af919059
1599862498,   18754115
```

Dadurch kann der Disk Manager-Prozess erkennen, welche Ereignisse bereits verarbeitet (an FMC gesendet) wurden und welche nicht.

Beachten Sie, dass der Datenträgermanager einheitliche Ereignisdateien löscht, wenn er ein Ereignissilo löscht. Weitere Informationen zum Abfluss von Silos finden Sie im Abschnitt Datenträgerverwaltung.

Eine entleerte, vereinheitlichte Datei gilt als nicht verarbeitet, wenn eines der folgenden Ereignisse zutrifft:

1. Der Zeitstempel des Lesezeichens ist kleiner als die Erstellungszeit der Datei.
2. Der Zeitstempel des Lesezeichens entspricht dem Zeitpunkt der Dateierstellung, und die Position in Byte in der Datei ist kleiner als ihre Größe.

Der EventHandler-Prozess liest Ereignisse aus den vereinheitlichten Dateien und überträgt sie (als Metadaten) über sftunnel an das FMC. Dieser Prozess ist für die verschlüsselte Kommunikation zwischen dem Sensor und dem FMC verantwortlich. Dies ist eine TCP-basierte Verbindung, sodass das Ereignis-Streaming vom FMC bestätigt wird.

Sie können diese Meldungen in der Datei [/ngfw]/var/log/messages sehen:

```
sfpreproc:OutputFile [INFO] *** Opening /ngfw/var/sf/detection_engines/77d31ce2-c2fc-11ea-b470-d428d53ed3ae/instance-1/unified_events-2.log.1597810478 for output" in /var/log/messages

EventHandler:SpoolIterator [INFO] Opened unified event file /var/sf/detection_engines/77d31ce2-c2fc-11ea-b470-d428d53ed3ae/instance-1/unified_events-2.log.1597810478

sftunneld:FileUtils [INFO] Processed 10334 events from log file var/sf/detection_engines/77d31ce2-c2fc-11ea-b470-d428d53ed3ae/instance-1/unified_events-2.log.1597810478
```

Diese Ausgabe enthält folgende Informationen:

- Snort hat die Datei unified_events für die Ausgabe geöffnet (um sie zu schreiben).
- Der Ereignishandler hat die gleiche Datei "unified_events" geöffnet (zum Lesen daraus).
- sftunnel hat die Anzahl von Ereignissen gemeldet, die von dieser Datei "unified_events" verarbeitet wurden.

Die Lesezeichendatei wird dann entsprechend aktualisiert. Der Sftunnel verwendet zwei verschiedene Kanäle, die als Unified Events (UE) Channel 0 und 1 für Ereignisse mit hoher bzw. niedriger Priorität bezeichnet werden.

Mit dem Befehl **sfunnel_status** CLI auf der FTD können Sie die Anzahl der gestreamten Ereignisse anzeigen.

```
Priority UE Channel 1 service

TOTAL TRANSMITTED MESSAGES <530541> for UE Channel service
RECEIVED MESSAGES <424712> for UE Channel service
SEND MESSAGES <105829> for UE Channel service
FAILED MESSAGES <0> for UE Channel service
HALT REQUEST SEND COUNTER <17332> for UE Channel service
STORED MESSAGES for UE Channel service (service 0/peer 0)
STATE <Process messages> for UE Channel service
REQUESTED FOR REMOTE <Process messages> for UE Channel service
REQUESTED FROM REMOTE <Process messages> for UE Channel service
```

Im FMC werden die Ereignisse vom SFDataCorrelator Prozess empfangen.

Der Status der Ereignisse, die von jedem Sensor verarbeitet wurden, kann mit dem Befehl

stats_unified.pl angezeigt werden:

```
admin@FMC:~$ sudo stats_unified.pl
Current Time - Fri Sep 9 23:00:47 UTC 2020

********************************************************************************
* FTD - 60a0526e-6ddf-11ea-99fa-89a415c16717, version 6.6.0.1
********************************************************************************
 Channel Backlog Statistics (unified_event_backlog)
   Chan    Last Time              Bookmark Time          Bytes Behind
      0    2020-09-09 23:00:30    2020-09-07 10:41:50               0
      1    2020-09-09 23:00:30    2020-09-09 22:14:58            6960
```

Dieser Befehl zeigt den Status des Rückstands von Ereignissen für ein bestimmtes Gerät pro Kanal an. Die verwendete Kanal-ID entspricht dem Sftunnel.

Der Bytes Behind-Wert kann als die Differenz zwischen der in der einheitlichen Ereignislesezeichendatei angezeigten Position und der Größe der einheitlichen Ereignisdatei sowie jeder nachfolgenden Datei mit einem höheren Zeitstempel als der in der Lesezeichendatei angegebenen berechnet werden.

Der SFDataCorrelator-Prozess speichert auch Leistungsstatistiken, die in **/var/sf/rna/correlator-stats/** gespeichert werden. Pro Tag wird eine Datei erstellt, in der die Leistungsstatistiken für diesen Tag im CSV-Format gespeichert werden. Der Name der Datei verwendet das Format "**JJJJ-MM-TT**" und die Datei, die dem aktuellen Tag entspricht, wird **jetzt** aufgerufen.

Die Statistiken werden alle 5 Minuten gesammelt (es gibt eine Zeile pro 5-Minuten-Intervall).

Die Ausgabe dieser Datei kann mit dem Befehl **perfstats** gelesen werden. Beachten Sie, dass dieser Befehl auch zum Lesen von SNORT-Leistungsstatistikdateien verwendet wird. Daher müssen die entsprechenden Flags verwendet werden:

C: Weist perfstats an, dass es sich bei der Eingabe um eine korrelator-stats-Datei handelt (ohne dieses Flag setzt perfstats voraus, dass es sich bei der Eingabe um eine snort-Leistungsstatistikdatei handelt).

-q: Ruhemodus: Es wird nur die Zusammenfassung für die Datei ausgegeben.

```
admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
287 statistics lines read

                host limit:                     50000           0               50000
                pcnt host limit in use:         100.01          100.00          100.55
                rna events/second:              1.22            0.00            48.65
                user cpu time:                  1.56            0.11            58.20
                system cpu time:                1.31            0.00            41.13
                memory usage:                   5050384         0               5138904
                resident memory usage:          801920          0               901424
                rna flows/second:               64.06           0.00            348.15
      rna dup flows/second:             0.00            0.00            37.05
                 ids alerts/second:              1.49            0.00             4.63
                ids packets/second:             1.71            0.00            10.10
                ids comm records/second:        3.24            0.00            12.63
                ids extras/second:              0.01            0.00            0.07
                fw_stats/second:                1.78            0.00            5.72
                user logins/second:             0.00            0.00            0.00
                 file events/second:             0.00            0.00             3.25
```

```
malware events/second:          0.00            0.00            0.06
fireamp events/second:          0.00            0.00            0.00
```

Jede Zeile in der Zusammenfassung hat drei Werte in dieser Reihenfolge: Durchschnitt, Minimum, Maximum.

Wenn Sie ohne das -q-Flag drucken, sehen Sie auch die 5-Minuten-Intervallwerte. Die Zusammenfassung wird am Ende angezeigt.

Beachten Sie, dass jedes FMC über eine maximale Flussrate verfügt, die in seinem Datenblatt beschrieben ist. Die nächste Tabelle enthält die Werte pro Modul aus dem jeweiligen Datenblatt:

Modell	FMC 750	FMC 1000	FMC 1600	FÜZ 2000	FMC 2500	FMC 2600	FMC 4000	FMC 4500	FMC 4600	FMCv	FMC
Maximale Durchsatzrate (fps)	2000	5000	5000	12000	12000	12000	20000	20000	20000	Variable	12

Beachten Sie, dass diese Werte für die Summe aller Ereignisarten stehen, die in der Statistikausgabe von SFDataCorrelator fett dargestellt werden.

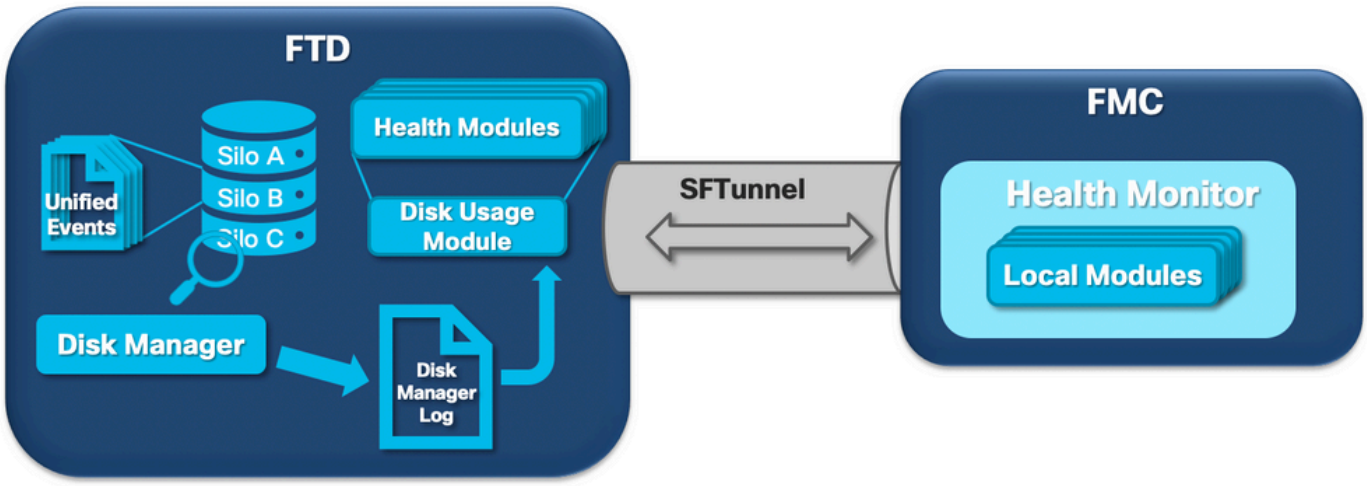
Wenn Sie sich die Ausgabe ansehen und wir unser FMC so bemessen, dass wir für das Worst-Case-Szenario vorbereitet sind (wenn alle Maximalwerte gleichzeitig auftreten), dann ist die Rate der Ereignisse, die dieses FMC erkennt, 48,65 + 348,15 + 4,63 + 3,25 + 0,06 = **404,74 fps** .

Dieser Gesamtwert kann mit dem Wert aus dem Datenblatt des jeweiligen Modells verglichen werden.

Der SFDataCorrelator kann zusätzlich zu den empfangenen Ereignissen arbeiten (z. B. für Korrelationsregeln), und speichert sie dann in der Datenbank, die abgefragt wird, um verschiedene Informationen in der grafischen Benutzeroberfläche (GUI) des FMC, z. B. Dashboards und Ereignisansichten, aufzufüllen.

Datenträgerverwaltung

Das nächste logische Diagramm zeigt die logischen Komponenten für den **Systemmonitor** und den **Datenträgermanager,** da sie für die Generierung von Datenträgerzustandswarnungen miteinander verflochten sind.



Kurz gesagt, der Disk-Manager-Prozess verwaltet die Festplattennutzung der Box und hat seine Konfigurationsdateien im Ordner [/ngfw]/etc/sf/. Es gibt mehrere Konfigurationsdateien für den Datenträgerverwaltungsprozess, die unter bestimmten Umständen verwendet werden:

- diskmanager.conf - Standardkonfigurationsdatei
- diskmanager_2hd.conf - Wird verwendet, wenn auf dem Gerät zwei Festplatten installiert sind. Die zweite Festplatte ist die mit der Malware-Erweiterung verbundene Festplatte, auf der Dateien gemäß der Dateirichtlinie gespeichert werden.
- ramdisk-diskmanager.conf - Wird verwendet, wenn "Log to Ramdisk" aktiviert ist. Weitere Informationen finden Sie im Abschnitt "Log to Ramdisk".

Jedem vom Datenträgermanager überwachten Dateityp wird ein Silo zugewiesen. Auf Basis des im System verfügbaren Festplattenspeichers berechnet der Festplattenmanager für jedes Silo eine Wassermarke (High Water Mark, HWM) und eine Wassermarke (Low Water Mark, LWM).

Wenn der Disk Manager-Prozess ein Silo entleert, tut er dies bis zum Erreichen des LWM. Da Ereignisse pro Datei entladen werden, kann dieser Schwellenwert überschritten werden.

Um den Status der Silos auf einem Sensorgerät zu überprüfen, können Sie folgenden Befehl verwenden:

```
> show disk-manager
Silo                                Used        Minimum     Maximum
misc_fdm_logs                       0 KB        65.208 MB   130.417 MB
Temporary Files                     0 KB        108.681 MB  434.726 MB
Action Queue Results                0 KB        108.681 MB  434.726 MB
User Identity Events                0 KB        108.681 MB  434.726 MB
UI Caches                           4 KB        326.044 MB  652.089 MB
Backups                             0 KB        869.452 MB  2.123 GB
Updates                             304.367 MB  1.274 GB    3.184 GB
Other Detection Engine              0 KB        652.089 MB  1.274 GB
Performance Statistics              45.985 MB   217.362 MB  2.547 GB
Other Events                        0 KB        434.726 MB  869.452 MB
IP Reputation & URL Filtering       0 KB        543.407 MB  1.061 GB
arch_debug_file                     0 KB        2.123 GB    12.736 GB
Archives & Cores & File Logs        0 KB        869.452 MB  4.245 GB
Unified Low Priority Events         974.109 MB  1.061 GB    5.307 GB
RNA Events                          879 KB      869.452 MB  3.396 GB
File Capture                        0 KB        2.123 GB    4.245 GB
Unified High Priority Events        252 KB      3.184 GB    7.429 GB
IPS Events                          3.023 MB    2.547 GB    6.368 GB
```

Der Datenträgerverwaltungsprozess wird ausgeführt, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Prozess wird gestartet (oder neu gestartet)
- Ein Silo erreicht die HWM
- Ein Silo wird manuell entleert
- Einmal pro Stunde

Jedes Mal, wenn der Disk Manager-Prozess ausgeführt wird, generiert er einen Eintrag für jedes der unterschiedlichen Silos in seiner eigenen Protokolldatei, die sich unter [/ngfw]/var/log/diskmanager.log befindet und Daten im CSV-Format enthält.

Als Nächstes wird eine Beispielzeile aus der Datei "diskmanager.log" angezeigt, die von einem Sensor stammt, der den Ablauf nicht verarbeiteter Ereignisse aus dem Systemzustand "Unified Low Priority Events" ausgelöst hat, sowie die Aufschlüsselung der entsprechenden Spalten:

```
priority_2_events,1599668981,221,4587929508,1132501868,20972020,4596,1586044534,5710966962,11421
93392,110,0
```

Spalte	Wert
Silo-Label	priority_2_events
Entleerungszeit (Epochenzeit)	1599668981
Anzahl der entleerten Dateien	221
Byte entladen	4587929508
Aktuelle Datengröße nach Ablauf (Byte)	1132501868
Größte entleerte Datei (Byte)	20972020
Kleinste entleerte Datei (Byte)	4596
Älteste entleerte Datei (Epochenzeit)	1586044534
Hohes Wasserzeichen (Byte)	5710966962
Niedrige Wasserzeichen (Byte)	1142193392
Anzahl der Dateien mit nicht verarbeiteten Ereignissen, die gelöscht wurden	110
Diskmanager-Zustandsflag	0

Diese Informationen werden dann vom jeweiligen Health Monitor-Modul gelesen, um den entsprechenden Health Alert auszulösen.

Manuelles Entleeren eines Silos

In bestimmten Szenarien können Sie ein Silo manuell entleeren. Wenn Sie z. B. Speicherplatz mit manueller Silo-Auslese anstatt manueller Dateientfernung freigeben möchten, hat der Datenträgermanager den Vorteil, dass er entscheiden kann, welche Dateien aufbewahrt und welche gelöscht werden sollen. Der Datenträgermanager speichert die neuesten Dateien für dieses Silo.

Jedes Silo kann entleert werden, und dies funktioniert wie bereits beschrieben (der Disk Manager entleert Daten, bis die Datenmenge unter den LWM-Grenzwert fällt). Der Befehl **system support silo-drain** ist im FTD CLISH-Modus verfügbar und bietet eine Liste der verfügbaren Silos (Name + numerische ID).

Dies ist ein Beispiel für eine manuelle Ableitung des Unified Low Priority Events-Silos:

```
> show disk-manager
Silo                                Used        Minimum     Maximum
misc_fdm_logs                       0 KB        65.213 MB   130.426 MB
Temporary Files                     0 KB        108.688 MB  434.753 MB
Action Queue Results                0 KB        108.688 MB  434.753 MB
User Identity Events                0 KB        108.688 MB  434.753 MB
UI Caches                           4 KB        326.064 MB  652.130 MB
Backups                             0 KB        869.507 MB  2.123 GB
Updates                             304.367 MB  1.274 GB    3.184 GB
Other Detection Engine              0 KB        652.130 MB  1.274 GB
Performance Statistics              1.002 MB    217.376 MB  2.547 GB
Other Events                        0 KB        434.753 MB  869.507 MB
```

```
IP Reputation & URL Filtering           0 KB        543.441 MB  1.061 GB
arch_debug_file                         0 KB        2.123 GB    12.737 GB
Archives & Cores & File Logs            0 KB        869.507 MB  4.246 GB
Unified Low Priority Events             2.397 GB    1.061 GB    5.307 GB
RNA Events                              8 KB        869.507 MB  3.397 GB
File Capture                            0 KB        2.123 GB    4.246 GB
Unified High Priority Events            0 KB        3.184 GB    7.430 GB
IPS Events                              0 KB        2.547 GB    6.368 GB

> system support silo-drain
Available Silos
  1 - misc_fdm_logs
  2 - Temporary Files
  3 - Action Queue Results
  4 - User Identity Events
  5 - UI Caches
  6 - Backups
  7 - Updates
  8 - Other Detection Engine
  9 - Performance Statistics
 10 - Other Events
 11 - IP Reputation & URL Filtering
 12 - arch_debug_file
 13 - Archives & Cores & File Logs
 14 - Unified Low Priority Events
 15 - RNA Events
 16 - File Capture
 17 - Unified High Priority Events
 18 - IPS Events
  0 - Cancel and return

Select a Silo to drain: 14
Silo Unified Low Priority Events being drained.

> show disk-manager
Silo                                    Used        Minimum     Maximum
misc_fdm_logs                           0 KB        65.213 MB   130.426 MB
Temporary Files                         0 KB        108.688 MB  434.753 MB
Action Queue Results                    0 KB        108.688 MB  434.753 MB
User Identity Events                    0 KB        108.688 MB  434.753 MB
UI Caches                               4 KB        326.064 MB  652.130 MB
Backups                                 0 KB        869.507 MB  2.123 GB
Updates                                 304.367 MB  1.274 GB    3.184 GB
Other Detection Engine                  0 KB        652.130 MB  1.274 GB
Performance Statistics                  1.002 MB    217.376 MB  2.547 GB
Other Events                            0 KB        434.753 MB  869.507 MB
IP Reputation & URL Filtering           0 KB        543.441 MB  1.061 GB
arch_debug_file                         0 KB        2.123 GB    12.737 GB
Archives & Cores & File Logs            0 KB        869.507 MB  4.246 GB
Unified Low Priority Events             1.046 GB    1.061 GB    5.307 GB
RNA Events                              8 KB        869.507 MB  3.397 GB
File Capture                            0 KB        2.123 GB    4.246 GB
Unified High Priority Events            0 KB        3.184 GB    7.430 GB
IPS Events                              0 KB        2.547 GB    6.368 GB
```

Zustandsüberwachung

Dies sind die wichtigsten Punkte:

- Alle Statusmeldungen, die im FMC im Menü für den Zustandsmonitor oder auf der Registerkarte für den Zustand im Nachrichtencenter angezeigt werden, werden vom Zustandsüberwachungsprozess generiert.

- Dieser Prozess überwacht den Zustand des Systems, sowohl für das FMC als auch für die verwalteten Sensoren, und besteht aus einer Reihe verschiedener Module.
- Integritätswarnmodule werden in der Integritätsrichtlinie definiert, die pro Gerät angehängt werden kann.
- Integritätswarnungen werden vom Modul "Datenträgerverwendung" generiert, das auf jedem vom FMC verwalteten Sensor ausgeführt werden kann.
- Wenn der Health Monitor-Prozess auf dem FMC ausgeführt wird (alle 5 Minuten oder bei Auslösung eines manuellen Vorgangs), prüft das Disk Usage-Modul die Datei "diskmanager.log", und wenn die richtigen Bedingungen erfüllt sind, wird die entsprechende Health Alert-Meldung ausgelöst.

Damit eine Statuswarnung **für das Ableiten nicht verarbeiteter Ereignisse** ausgelöst wird, müssen alle folgenden Bedingungen erfüllt sein:

1. Das Feld Bytes drained ist größer als 0 (dies zeigt an, dass Daten aus diesem Silo drained waren).
2. Die Anzahl der Dateien mit nicht verarbeiteten Ereignissen, deren Drain-Wert größer als 0 ist (dies zeigt an, dass in den drainierten Daten nicht verarbeitete Ereignisse aufgetreten sind).
3. Die Zeit der Entleerung ist innerhalb der letzten 1 Stunde.

Damit eine **Warnung** über **die** Systemintegrität bei **häufigem Abfluss von Ereignissen** ausgelöst wird, müssen die folgenden Bedingungen zutreffen:

1. Die letzten beiden Einträge in der Datei diskmanager.log müssen: Feld für abgelaufene Bytes größer als 0 (gibt an, dass Daten aus diesem Silo abgelaufen sind).Der Abstand sollte weniger als 5 Minuten betragen.
2. Der Zeitpunkt der Entleerung des letzten Eintrags für dieses Silo ist innerhalb der letzten 1 Stunde.

Die Ergebnisse aus dem Festplattennutzungsmodul (sowie die von den anderen Modulen gesammelten Ergebnisse) werden über Sftunnel an das FMC gesendet. Mit dem Befehl **sftunnel_status** können Sie Zähler für die Systemereignisse anzeigen, die über sftunnel ausgetauscht werden:

```
TOTAL TRANSMITTED MESSAGES <3544> for Health Events service
RECEIVED MESSAGES <1772> for Health Events service
SEND MESSAGES <1772> for Health Events service
FAILED MESSAGES <0> for Health Events service
HALT REQUEST SEND COUNTER <0> for Health Events service
STORED MESSAGES for Health service (service 0/peer 0)
STATE <Process messages> for Health Events service
REQUESTED FOR REMOTE <Process messages> for Health Events service
REQUESTED FROM REMOTE <Process messages> for Health Events service
```

Bei Ramdisk anmelden

Obwohl die meisten Ereignisse auf der Festplatte gespeichert sind, ist das Gerät standardmäßig so konfiguriert, dass es sich bei Ramdisk anmeldet, um eine allmähliche Beschädigung der SSD zu verhindern, die durch ständige Schreibvorgänge und Löschungen von Ereignissen auf der Festplatte verursacht werden kann.

In diesem Szenario werden die Ereignisse nicht unter **[/ngfw]/var/sf/detection_engine/*/instance-N/ gespeichert,** sondern befinden sich in **[/ngfw]/var/sf/detection_engines/*/instance-N/connection/**,

was eine symbolische Verbindung zu **/dev/shm/instance-**ist N/Verbindung. In diesem Fall befinden sich die Ereignisse nicht im physischen, sondern im virtuellen Speicher.

```
admin@FTD4140:~$ ls -la /ngfw/var/sf/detection_engines/b0c4a5a4-de25-11ea-8ec3-
4df4ea7207e3/instance-1/connection
lrwxrwxrwx 1 sfsnort sfsnort 30 Sep  9 19:03 /ngfw/var/sf/detection_engines/b0c4a5a4-de25-11ea-
8ec3-4df4ea7207e3/instance-1/connection -> /dev/shm/instance-1/connection
```

Um zu überprüfen, was das Gerät derzeit konfiguriert ist, führen Sie den Befehl **show log-events-to-ramdisk** aus der FTD-CLISH aus. Sie können dies auch ändern, wenn Sie den Befehl **configure log-events-to-ramdisk <enable/disable> verwenden:**

```
> show log-events-to-ramdisk
Logging connection events to RAM Disk.

>configure log-events-to-ramdisk
Enable or Disable  enable or disable (enable/disable)
```

> **Warnung:** Wenn der Befehl "configure log-events-to-ramdisk disable" ausgeführt wird, müssen auf dem FTD zwei Bereitstellungen durchgeführt werden, damit snort nicht im Zustand "D" (Unterbrechungsfreier Energiesparmodus) feststeckt, was zu Datenverkehrsausfällen führen würde.
> Dieses Verhalten wird im Defekt mit der Cisco Bug-ID CSCvz53372 dokumentiert. Bei der ersten Bereitstellung wird die Neubewertung der Snort-Speicherphase übersprungen, was dazu führt, dass Snort in den "D"-Zustand versetzt wird. Die Problemumgehung besteht darin, eine weitere Bereitstellung mit etwaigen Dummy-Änderungen durchzuführen.

Wenn Sie sich bei ramdisk einloggen, ist der Hauptnachteil, dass das jeweilige Silo einen kleineren Platz hat und sie somit unter den gleichen Umständen öfter entwässert. Die nächste Ausgabe ist der Disk Manager von einem FPR 4140 mit und ohne die Log-Ereignisse zu ramdisk aktiviert für den Vergleich.

Protokoll auf Ramdisk aktiviert

```
> show disk-manager
Silo                                Used        Minimum     Maximum
Temporary Files                     0 KB        903.803 MB  3.530 GB
Action Queue Results                0 KB        903.803 MB  3.530 GB
User Identity Events                0 KB        903.803 MB  3.530 GB
UI Caches                           4 KB        2.648 GB    5.296 GB
Backups                             0 KB        7.061 GB    17.652 GB
Updates                             305.723 MB  10.591 GB   26.479 GB
Other Detection Engine              0 KB        5.296 GB    10.591 GB
Performance Statistics              19.616 MB   1.765 GB    21.183 GB
Other Events                        0 KB        3.530 GB    7.061 GB
IP Reputation & URL Filtering       0 KB        4.413 GB    8.826 GB
arch_debug_file                     0 KB        17.652 GB   105.914 GB
Archives & Cores & File Logs        0 KB        7.061 GB    35.305 GB
RNA Events                          0 KB        7.061 GB    28.244 GB
File Capture                        0 KB        17.652 GB   35.305 GB
Unified High Priority Events        0 KB        17.652 GB   30.892 GB
Connection Events                   0 KB        451.698 MB  903.396 MB
IPS Events                          0 KB        12.357 GB   26.479 GB
```

Protokoll auf Ramdisk deaktiviert

```
> show disk-manager
Silo                                Used        Minimum     Maximum
Temporary Files                     0 KB        976.564 MB  3.815 GB
Action Queue Results                0 KB        976.564 MB  3.815 GB
User Identity Events                0 KB        976.564 MB  3.815 GB
UI Caches                           4 KB        2.861 GB    5.722 GB
Backups                             0 KB        7.629 GB    19.074 GB
Updates                             305.723 MB  11.444 GB   28.610 GB
Other Detection Engine              0 KB        5.722 GB    11.444 GB
Performance Statistics              19.616 MB   1.907 GB    22.888 GB
Other Events                        0 KB        3.815 GB    7.629 GB
IP Reputation & URL Filtering       0 KB        4.768 GB    9.537 GB
arch_debug_file                     0 KB        19.074 GB   114.441 GB
Archives & Cores & File Logs        0 KB        7.629 GB    38.147 GB
Unified Low Priority Events         0 KB        9.537 GB    47.684 GB
RNA Events                          0 KB        7.629 GB    30.518 GB
File Capture                        0 KB        19.074 GB   38.147 GB
Unified High Priority Events        0 KB        19.074 GB   33.379 GB
IPS Events                          0 KB        13.351 GB   28.610 GB
```

Die kleinere Größe des Silos wird durch die höhere Geschwindigkeit kompensiert, mit der auf die Ereignisse zugegriffen und diese an das FMC übertragen werden können. Dies ist zwar unter angemessenen Bedingungen eine bessere Option, der Nachteil muss jedoch berücksichtigt werden.

Häufig gestellte Fragen

Werden die Integritätswarnungen bei Ablauf von Ereignissen nur von Verbindungsereignissen generiert?

Nein.

- Alerts of Frequent Drain können von jedem Disk Manager Silo generiert werden.
- Warnungen über den Ablauf nicht verarbeiteter Ereignisse können von jedem ereignisbezogenen Silo generiert werden.

Verbindungsereignisse sind die häufigsten Ursachen.

Ist es immer ratsam, Log to Ramdisk zu deaktivieren, wenn eine Warnung über den Zustand häufiger Abflüsse angezeigt wird?

Nein. Nur in Szenarien mit übermäßiger Protokollierung außer DOS/DDOS, wenn das betroffene Silo das Verbindungsereignissilo ist, und nur in Fällen, in denen es nicht möglich ist, die Protokollierungseinstellungen weiter anzupassen.

Wenn DOS/DDOS übermäßige Protokollierung verursacht, besteht die Lösung darin, DOS/DDOS-Schutz zu implementieren oder die Quelle(n) der DOS/DDOS-Angriffe zu beseitigen.

Die Standardfunktion "Log to Ramdisk" reduziert den SSD-Verschleiß, daher wird dringend empfohlen, sie zu verwenden.

Was ist ein nicht bearbeitetes Ereignis?

Ereignisse werden nicht einzeln als nicht verarbeitet markiert. Eine Datei hat nicht verarbeitete Ereignisse, wenn:

Sein Erstellungszeitstempel ist höher als das Zeitstempelfeld in der jeweiligen Lesezeichendatei.

Oder

Sein Erstellungszeitstempel entspricht dem Zeitstempelfeld in der jeweiligen Lesezeichendatei und seine Größe ist größer als die Position im Byte-Feld in der jeweiligen Lesezeichendatei.

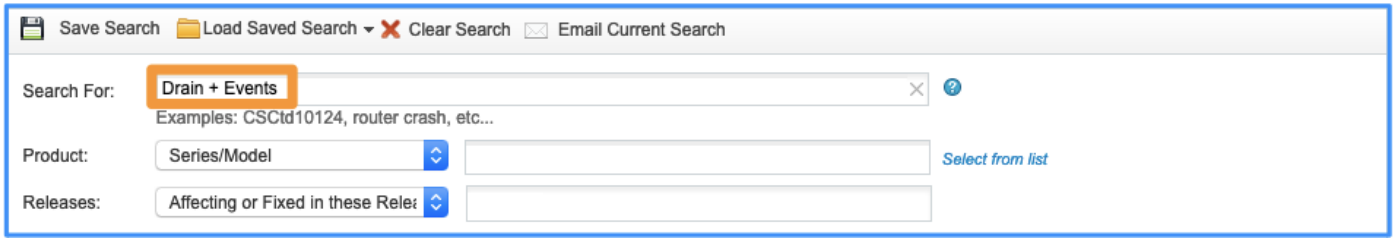
Woher weiß das FMC die Anzahl der Bytes, die für einen bestimmten Sensor zurückliegen?

Der Sensor sendet Metadaten über den Dateinamen und die Größe der Unified_events-Datei sowie die Informationen über die Lesezeichendateien, wodurch das FMC genügend Informationen erhält, um die Bytes zu berechnen, die sich hinter den Dateien befinden:

Aktuelle Unified_events-Dateigröße - **Position in Bytes"-**Feld aus Lesezeichendatei + Größe aller Unified_events-Dateien mit einem höheren Zeitstempel als dem Zeitstempel in der jeweiligen Lesezeichendatei.

Bekannte Probleme

Öffnen Sie das Bug Search Tool und verwenden Sie diese Abfrage:



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.